TD 2. Éléments primitifs et résidus quadratiques

Exercice 1 (Éléments primitifs)

1. a) Montrer que 2 est un élément primitif modulo 29.
   b) Quels sont les ordres possibles des éléments de $(\mathbb{Z}/29\mathbb{Z})^*$? En déduire la liste des puissances de 2 qui sont des éléments primitifs modulo 29.
   c) Résoudre l'équation $x^7 \equiv 1 \mod 29$.
2. Déterminer de même les éléments primitifs modulo 11 et 13.
3. Soit p un premier impair.
   a) On suppose p congru à 1 modulo 4, montrer que a est un élément primitif modulo p si et seulement si $-a$ est un élément primitif modulo p.
   [Pour ($\Rightarrow$), on pourra considérer un entier ℓ tel que $(-a)^\ell \equiv 1 \mod p$ et voir ce que cela entraîne pour a^ℓ selon que ℓ est pair ou impair.]
   b) On suppose p congru à 3 modulo 4, montrer que a est un élément primitif modulo p si et seulement si $-a$ est d'ordre $\frac{p-1}{2}$ dans $(\mathbb{Z}/p\mathbb{Z})^*$.
   [Pour ($\Leftarrow$), on établira l'implication : $\forall \ell \in \mathbb{Z},\ a^\ell \equiv 1 \mod p \Rightarrow \frac{p-1}{2} \mid \ell$ et on vérifiera qu'elle entraîne que $\frac{p-1}{2}$ divise l'ordre de a.]
   c) Soit a un élément primitif modulo p^2. Montrer que a est un élément primitif modulo p.

Exercice 2 (Wilson)

Soit p un nombre premier.

1. Donner une nouvelle preuve du théorème de Wilson :
$$(p-1)! \equiv -1 \mod p \ .$$
en utilisant l'existence d'un élément primitif a modulo p.
2. Soit $\mathcal{R}$ l'ensemble des entiers compris entre 1 et $p-1$ qui sont *résidus quadratiques* modulo p (c'est-à-dire congrus à un carré modulo p). Montrer de façon analogue à ci-dessus que le produit des éléments de $\mathcal{R}$ est congru modulo p à :
$$\begin{cases} 1 & \text{si } p = 2 \text{ ou } p \equiv 3 \mod 4, \\ -1 & \text{sinon.} \end{cases}$$
Qu'en est-il du produit des entiers compris entre 1 et $p-1$ qui ne sont pas résidus quadratiques modulo p ?

Exercice 3 (Racines carrées)
Soit p un nombre premier.

1. Vérifier que :
   a) $\displaystyle\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)=0$;
   b) pour $a\in\mathbb{Z}$, le nombre de solutions de $x^2\equiv a \mod p$ est égal à $1+\left(\frac{a}{p}\right)$.
2. a) En déduire que le nombre N de solutions de $x^2-y^2\equiv a \mod p$ est $\displaystyle p+\sum_{y=0}^{p-1}\left(\frac{y^2+a}{p}\right)$.
   b) Utiliser le changement de variables $u=x+y$, $v=x-y$ pour trouver une autre expression de N (on traitera séparément les deux cas $(a,p)=1$ et $p\,|\,a$).
   c) En déduire que :
$$\sum_{y=0}^{p-1}\left(\frac{y^2+a}{p}\right)=\begin{cases}-1 & \text{si } a \text{ est premier à } p,\\ p-1 & \text{si } p\,|\,a.\end{cases}$$
3. On suppose p impair et a premier à p.
   a) Montrer que le nombre de solutions de $ax^2+bx+c\equiv 0 \mod p$ est égal à $1+\left(\frac{b^2-4ac}{p}\right)$.
   b) Soit $b\in\mathbb{Z}$, que vaut $\displaystyle\sum_{x=0}^{p-1}\left(\frac{ax+b}{p}\right)$?

Exercice 4 (Symbole de Legendre)
a) Déterminer à l'aide de la loi de réciprocité quadratique les premiers impairs p tels que 7 soit un carré modulo p. Faire de même pour 15.
b) Soit p un premier impair avec $p\equiv 1 \mod 3$, montrer que $(\mathbb{Z}/p\mathbb{Z})^*$ contient un élément x d'ordre 3. Vérifier que $(2x+1)^2\equiv -3 \mod p$, en déduire la valeur de $\left(\frac{-3}{p}\right)$.
c) Faire de même quand $p\equiv 1 \mod 5$ (on calculera $(x+x^4)^2+(x+x^4)-1$ modulo p, où x est d'ordre 5).

Exercice 5 (Théorème Chinois des restes)
1. On rappelle que l'*indicateur de Carmichael* d'un entier n est l'e*xposant* de $(\mathbb{Z}/n\mathbb{Z})^*$.
   a) Donner la décomposition en facteurs premiers de 561 ;
   b) à l'aide du théorème chinois des restes, en déduire la structure de $(\mathbb{Z}/561\mathbb{Z})^*$;
   c) donner enfin les valeurs de l'indicateur d'Euler $\varphi(561)$ et de celui de Carmichael $\lambda(561)$.
2. Soit D un entier naturel impair et sans facteur carré.
   a) Montrer qu'il existe $b\in\mathbb{Z}$ tel que $\left(\frac{b}{D}\right)=-1$.
   b) On note $\varphi=\varphi(D)$ et $a_1,a_2,\ldots,a_\varphi$ des entiers représentants les éléments de $(\mathbb{Z}/D\mathbb{Z})^*$. Montrer qu'on a :
$$\sum_{i=1}^{\varphi}\left(\frac{a_i}{D}\right)=0 \ .$$
   En déduire qu'exactement la moitié des éléments a de $(\mathbb{Z}/D\mathbb{Z})^*$ vérifient $\left(\frac{a}{D}\right)=1$.
   c) Soit p un premier impair avec $(p,D)=1$ et $p\equiv 1 \mod 4$. Montrer que $\left(\frac{D}{p}\right)=1$ si et seulement si il existe i tel que $p\equiv a_i \mod D$ et $\left(\frac{a_i}{D}\right)=1$.
   d) Qu'en est-il si $p\equiv 3 \mod 4$?